On the "Security analysis and improvements of arbitrated quantum signature schemes"

Song-Kong Chong, Yi-Ping Luo, Tzonelih Hwang*

January 20, 2013

Abstract

Recently, Zou et al. [Phys. Rev. A 82, 042325 (2010)] pointed out that two arbitrated quantum signature (AQS) schemes are not secure, because an arbitrator cannot arbitrate the dispute between two users when a receiver repudiates the integrity of a signature. By using a public board, they try to propose two AQS schemes to solve the problem. This work shows that the same security problem may exist in their schemes and also a malicious party can reveal the other party's secret key without being detected by using the Trojan-horse attacks. Accordingly, two basic properties of a quantum signature, i.e. unforgeability and undeniability, may not be satisfied in their scheme.

Keywords: Quantum information; Quantum cryptography; Arbitrated quantum signature.

1 Introduction

Quantum signature, which concerns about the authenticity and non-repudiation of quantum states on an insecure quantum channel [1, 2], is one of the most

*Corresponding Author

important researches in quantum cryptography. By exploiting the principles of quantum mechanics, e.g., no-cloning theory and measurement uncertainty, quantum signature can provide unconditional security. Two basic properties are required in a quantum signature [1] :

1. Unforgeability: Neither the signature verifier nor an attacker can forge a signature, or change or attach the content of a signature. The signature should not be reproduced by any other person.

2. Undeniability: A signatory, Alice, who has sent the signature to the verifier, Bob, cannot later deny having signed a signature. Moreover, the verifier Bob cannot deny the receipt of the signature.

Quantum signature was first investigated by Gottesman and Chuang [3]. After that, a variety of quantum signature schemes have been proposed [1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]. Zeng et al. [1] proposed an arbitrated quantum signature (AQS) scheme based on the correlation of GHZ states and quantum one-time pads. However, Curty et al. [6] pointed out that [1] is not clearly described and the security statements claimed by the authors are incorrect. In the reply comment [7], Zeng gave a more detailed presentation and proof to their original AQS scheme [1]. To improve the transmission efficiency and to reduce the implementation complexity of [1, 7], Li et al. [8] proposed an AQS scheme using Bell states and claimed that their improvements can preserve the merits in the original scheme [1, 7].

In an AQS scheme, an arbitrator plays a crucial role. When a dispute arises between the users, the arbitrator should be able to arbitrate the dispute. The arbitrator should be able to solve a dispute when a receiver, Bob, repudiates the receipt of the signature, or in particular, the receiver repudiates the integrality of the signature, i.e., Bob admits receiving a signature but denies the correctness of the signature. The dispute of the latter one implies the following three cases

[15]:

(1) Bob told a lie;

(2) The signatory Alice sent incorrect information to Bob;

(3) An eavesdropper Eve disturbed the communications.

Since the arbitrator in [1, 7, 8] cannot solve the dispute when Bob claims that the verification of a signature is not successful, Zou et al. [15] considered that these schemes are not valid because the security requirement of a quantum signature, i.e., the undeniability, is not satisfied.

By using a public board, Zou et al. also proposed two AQS schemes to solve the problem. However, this study will point out that the same security problem may exist in their schemes. That is, when Bob announces that the verification is not successful, the arbitrator may not be able to distinguish which case described above has happened. Besides, this study also tries to investigate if a malicious signer, Alice, can reveal Bob's secret key without being detected by performing the Trojan-horse attacks [16, 17].

The rest of this paper is organized as follows. Section 2 reviews Zou et al.'s schemes. Section 3 shows the problems with the schemes. Finally, Section 4 concludes the result.

2 Review of Zou et al.'s schemes

Zou et al.'s AQS schemes [15] are briefly explained in the following scenario. Alice, the message signatory, would like to sign a quantum message $|P\rangle$ to a signature verifier, Bob, via the assistance of an arbitrator, Trent. Suppose that Alice and Bob share a secret key $K \in \{0,1\}^*$, and the quantum message to be signed is $|P\rangle = |P_1\rangle \otimes |P_2\rangle \otimes ... \otimes |P_n\rangle$, where $|K| \geq 2n$, $|P_i\rangle = \alpha_i |0\rangle + \beta_i |1\rangle$, and $1 \leq i \leq n$. In order to protect the quantum message, the quantum one-time-pad

encryption E_K [18] and the unitary transformation M_K used in the schemes are defined as follows.

$$E_K\left(|P\rangle\right) = \bigotimes_{i=1}^{n} \sigma_x^{K_{2i-1}} \sigma_z^{K_{2i}} \left|P_i\right\rangle, \tag{1}$$

$$M_K\left(|P\rangle\right) = \bigotimes_{i=1}^{n} \sigma_x^{K_i} \sigma_z^{K_{i\oplus 1}} \left|P_i\right\rangle, \tag{2}$$

where $|P_i\rangle$ and K_i denote the ith bit of $|P\rangle$ and K, σ_x and σ_z are the Pauli matrices, respectively.

To prevent the integrality of a signature from being disavowed by Bob, Zou et al. proposed two AQS schemes: the AQS scheme using Bell states and the AQS without using entangled states, respectively. Their schemes are described as follows.

2.1 Scheme 1: the AQS scheme using Bell states

Suppose that Alice wants to sign an n-bit quantum message $|P\rangle$ to Bob. In order to perform the signature, three copies of $|P\rangle$ are necessary. The scheme proceeds as follows:

Initializing phase:

Step *I*1. The arbitrator Trent shares the secret keys K_A, K_B with Alice and Bob respectively through some unconditionally secure quantum key distribution protocols.

Step *I*2. Alice generates n Bell states, $|\psi_i\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$, where $1 \leq i \leq n$, and the subscripts A and B denote the 1^{st} and the 2^{nd} particles of that Bell state, respectively. After that, Alice sends all B particles to Bob in a secure and authenticated way [19, 20].

Signing phase

Step $S\mathbf{1}$. Alice chooses a random number $r \in \{0,1\}^{2n}$ to encrypt all $|P\rangle$'s, i.e., $|P'\rangle = E_r(|P\rangle)$.

Step $S\mathbf{2}$. Alice generates $|S_A\rangle = E_{K_A}(|P'\rangle)$.

Step $S\mathbf{3}$. Alice combines each $|P_i'\rangle$ and the Bell state to obtain a three-particle entangled state,

$$|\phi_i\rangle = |P_i'\rangle \otimes |\psi_i\rangle_{AB} = \frac{1}{2}\left[\begin{array}{c} \left|\Phi_{PA}^{+}\right\rangle_i \left(\alpha_i'|0\rangle + \beta_i'|1\rangle\right)_B + \left|\Phi_{PA}^{-}\right\rangle_i \left(\alpha_i'|0\rangle - \beta_i'|1\rangle\right)_B + \\ \left|\Psi_{PA}^{+}\right\rangle_i \left(\alpha_i'|1\rangle + \beta_i'|0\rangle\right)_B + \left|\Psi_{PA}^{-}\right\rangle_i \left(\alpha_i'|1\rangle - \beta_i'|0\rangle\right)_B \end{array}\right],$$

where $\left|\Phi_{PA}^{+}\right\rangle, \left|\Phi_{PA}^{-}\right\rangle, \left|\Psi_{PA}^{+}\right\rangle$, and $\left|\Psi_{PA}^{-}\right\rangle$ are the four Bell states [21].

Step $S\mathbf{4}$. Alice performs a Bell-measurement on each $|\phi_i\rangle$ and obtains the measurement results $|M_A\rangle = \left(\left|M_A^1\right\rangle, \left|M_A^2\right\rangle, \ldots, |M_A^n\rangle\right)$, where $\left|M_A^i\right\rangle \in \left\{\left|\Phi_{PA}^{+}\right\rangle_i, \left|\Phi_{PA}^{-}\right\rangle_i, \left|\Psi_{PA}^{+}\right\rangle_i, \left|\Psi_{PA}^{-}\right\rangle_i\right\}$, and $1 \le i \le n$.

Step $S\mathbf{5}$. Alice sends $|S\rangle = (|P'\rangle, |S_A\rangle, |M_A\rangle)$ to Bob.

Verification phase:

Step $V\mathbf{1}$. Bob encrypts $|P'\rangle$ and $|S_A\rangle$ with K_B and sends the quantum ciphertext $|Y_B\rangle = E_{K_B}(|P'\rangle, |S_A\rangle)$ to Trent.

Step $V\mathbf{2}$. Trent decrypts $|Y_B\rangle$ with K_B and obtains $|P'\rangle$ and $|S_A\rangle$. Then he encrypts $|P'\rangle$ with K_A and gets $|S_T\rangle$. If $|S_T\rangle = |S_A\rangle$ [8, 22], Trent sets the verification parameter $V = 1$; otherwise, $V = 0$.

Step $V\mathbf{3}$. Trent recovers $|P'\rangle$ from $|S_T\rangle$. Then he encrypts $|P'\rangle, |S_A\rangle$ and V with K_B and sends the quantum ciphertext $|Y_T\rangle = E_{K_B}(|P'\rangle, |S_A\rangle, V)$ to Bob.

Step $V\mathbf{4}$. Bob decrypts $|Y_T\rangle$ and gets $|P'\rangle, |S_A\rangle$, and V. If $V = 0$, Bob rejects the signature; otherwise, Bob continues to the next step.

Step $V\mathbf{5}$. Based on Alice's measurement results M_A, Bob can obtain $|P'_B\rangle$ from the B particles received from the Step $I\mathbf{2}$ according to the principle of teleportation [8]. Then he compares $|P'_B\rangle$ with $|P'\rangle$. If $|P'_B\rangle = |P'\rangle$, Bob informs Alice to publish r and proceeds to the next step; otherwise, he rejects the signature.

Step $V\mathbf{6}$. Alice publishes r on the public board.

Step $V\mathbf{7}$. Bob recovers $|P\rangle$ from $|P'\rangle$ by r and holds $(|S_A\rangle, r)$ as Alice's signature for the quantum message $|P\rangle$.

2.2 Scheme 2: the AQS scheme without using entangled states

Since the preparation, distribution, and storing of quantum entangled states are not easily implemented with today's technologies, Zou et al. also proposed an AQS scheme without using entangled states (Scheme 2) in the signing phase and the verifying phase. In order to prevent a signature from being disavowed by Bob, a public board is also used in the proposed scheme. The scheme is described as follows.

Initializing phase:

Step $I\mathbf{1}'$. The arbitrator Trent shares the secret keys K_{AT}, K_{BT} with Alice and Bob respectively through some unconditionally secure quantum key distribution protocols. Similarly, Alice shares a secret key, K_{AB}, with Bob.

Signing phase:

Step $S\mathbf{1}'$. Alice chooses a random number $r \in \{0,1\}^{2n}$ and then computes $|P'\rangle = E_r(|P\rangle)$ and $|R_{AB}\rangle = M_{K_{AB}}(|P'\rangle)$, where $|P\rangle$ is as defined before.

Step $S\mathbf{2}'$. Alice generates $|S_A\rangle = E_{K_{AT}}(|P'\rangle)$.

Step $S\mathbf{3}'$. Alice generates $|S\rangle = E_{K_{AB}}(|P'\rangle, |R_{AB}\rangle, |S_A\rangle)$ as her signature and then sends it to Bob.

Verification phase:

Step $V\mathbf{1}'$. Bob decrypts $|S\rangle$ with K_{AB} and obtains $|P'\rangle, |R_{AB}\rangle$ and $|S_A\rangle$. Then he generates $|Y_B\rangle = E_{K_{BT}}(|P'\rangle, |S_A\rangle)$ and sends it to Trent.

Step $V\mathbf{2}'$. Trent decrypts $|Y_B\rangle$ with K_{BT} and obtains $|P'\rangle$ and $|S_A\rangle$.

Step $V\mathbf{3}'$. Trent decrypts $|S_A\rangle$ with K_{AT} to obtain $|P'_T\rangle$. If $|P'_T\rangle = |P'\rangle$, he sets the verification parameter $V_T = 1$; otherwise, $V_T = 0$. Then Trent announces V_T on the public board. If $V_T = 1$, he regenerates $|Y_B\rangle$ and sends it back to Bob.

Step $V\mathbf{4}'$. If $V_T = 0$, Bob rejects the signature. For otherwise, he decrypts $|Y_B\rangle$ with K_{BT} to obtain $|P'\rangle$ and $|S_A\rangle$. Then he computes $|P'_B\rangle = M^{-1}_{K_{AB}}(|R_{AB}\rangle)$ and compares it with $|P'\rangle$. If $|P'_B\rangle = |P'\rangle$, he sets the verification parameter $V_B = 1$; otherwise, $V_B = 0$. Bob announces V_B on the public board.

Step $V\mathbf{5}'$. If $V_B = 0$, Alice and Trent abort the scheme; otherwise, Alice announces r on the public board.

Step $V\mathbf{6}'$. Bob recovers $|P\rangle$ from $|P'\rangle$ by r and holds $(|S_A\rangle, r)$ as Alice's signature for the quantum message $|P\rangle$.

3 Problems to be discussed

This section tries to investigate problems that could arise on Zou et al.'s schemes if precautions are not taken. We first discuss the deniable dilemma. Then, we

investigate the Trojan-horse attacks against the schemes.

3.1 The deniable dilemma

In Zou et al.'s schemes, the signatory Alice uses a random number r to protect the quantum message $|P\rangle$ (i.e., $|P'\rangle = E_r(|P\rangle)$) before signing it. After the arbitrator Trent's verification, Bob recovers $|P'_B\rangle$ and compares it with $|P'\rangle$. Once Bob informs Alice that $|P'_B\rangle = |P'\rangle$, Alice will publish r on the public board, which is assumed to be free from being blocked, injected or alternated. Finally, Bob recovers $|P\rangle$ from $|P'\rangle$ by r and retains $(|S_A\rangle, r)$ as Alice's signature.

It appears that if Bob informs Alice to publish r on the public board, then he cannot disavow the integrality of the signature. Accordingly, Zou et al. considered that the use of the public board can prevent the denial attack from Bob. However, if Bob claims that $|P'_B\rangle \neq |P'\rangle$ in Step V5 (or Step V4' in Scheme 2), Trent cannot arbitrate the dispute between Alice and Bob because the following three cases are possible. (This is particularly serious, if the signature scenario occurs in an electronic block market, where Alice is a buyer and Bob, a block company.)

1. Bob told a lie: In this case, Bob decides to forgo the recovery of the message $|P\rangle$ due to some unknown reasons;

2. Alice sent incorrect information to Bob: In Step S3 of Scheme 1, Alice deliberately generated $|\phi_i\rangle$ by another message $\left|\hat{P}'_i\right\rangle$ with $\left|\hat{P}'_i\right\rangle \neq |P'_i\rangle$ or generated $|S\rangle = (|P'\rangle, |S_A\rangle, |M'_A\rangle)$ with $|M'_A\rangle \neq |M_A\rangle$ in Step S5. In Scheme 2, Alice intentionally sent $|S\rangle = E_{K_{AB}}\left(|P'\rangle, \left|\hat{R}_{AB}\right\rangle, |S_A\rangle\right)$ with $\left|\hat{R}_{AB}\right\rangle \neq |R_{AB}\rangle$ to Bob in Step S3';

3. Eve disturbed the communication.

Apparently, when Bob claims that $|P'_B\rangle \neq |P'\rangle$, Trent cannot solve the dispute.

Furthermore, as also pointed out in [15], the signer, Alice, is able to publish an arbitrary r' ($\neq r$) in her favor without been verified, which is obviously against the requirement of a signature scheme.

3.2 The Trojan-horse attack

In Zou et al.'s schemes, there are two transmissions of the same quantum signals, i.e. first from Alice to Bob, and then from Bob to the arbitrator. Therefore, the malicious Alice can reveal Bob's secret key without being detected by performing the Trojan-horse attacks [16, 17]. Similar to [5], there are two attack strategies in the Trojan-horse attacks: the invisible photon eavesdropping [16] and the delay photon eavesdropping [17]. The following will discuss the invisible photon eavesdropping (IPE) on Zou et al.'s schemes and show that Alice can obtain Bob's secret key without being detected. Note that, Alice can also use the delay photon eavesdropping to reveal Bob's secret key in the same way.

In Scheme 1, in order to reveal Bob's secret key K_B, Alice can perform the IPE attack on the communications in Step $S5$ and Step $V1$ as follows:

Step $S5$a. Alice first prepares a set of eavesdropping states, $D^i \in \left\{ \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)_{d_1^i d_2^i} \right\}$, as invisible photons, where the subscripts d_1^i and d_2^i represent the 1^{st} and 2^{nd} photons in D^i, $1 \leq i \leq n$. For each state in $|P'\rangle$ (or $|S_A\rangle$), Alice inserts d_1^i as an invisible photon to that state and forms a new sequence $|P'\rangle^{d_1}$ ($|S_A\rangle^{d_1}$). Then Alice sends $|S\rangle^{d_1} = \left(|P'\rangle^{d_1}, |S_A\rangle, |M_A\rangle\right)$ to Bob.

Step $V1$a. Bob encrypts $|P'\rangle^{d_1}$ and $|S_A\rangle$ with K_B and sends the quantum ciphertext $|Y_B\rangle^{d_{1'}} = E_{K_B}(|P'\rangle^{d_1}, |S_A\rangle)$ to Trent. Before Trent receives the quantum ciphertext $|Y_B\rangle^{d_{1'}}$, Alice captures $d_{1'}$ from $|Y_B\rangle^{d_{1'}}$ and measures $d_{1'}d_2$ together with the Bell measurement. According to the measuring result of $d_{1'}^i d_2^i$, Alice can obtain Bob's secret key $K_B^{2i-1,2i}$.

Note that, Alice can also use the similar ways mentioned above to obtain Bob's secret key K_{BT} in Scheme 2. Since both Scheme 1 and 2 are insecure to the Trojan-horse attacks, Bob can deny having verified a signature. Therefore, the basic properties of a quantum signature, i.e. unforgeability and undeniability, are not satisfied in their schemes.

4 Conclusions

This study has pointed out two security flaws in Zou et al.'s AQS schemes, in which the arbitrator cannot arbitrate the dispute between Alice and Bob when Bob claims failure in his verification. Besides, a malicious signer can obtain verifier's secret key by performing the Trojan-horse attacks. How to improve their AQS schemes to avoid the problems mentioned in this paper will be an interesting future research.

Acknowledgment

This research is supported partially by National Science Council, Taiwan, R.O.C., under the Contract No. NSC 98-2221-E006-097-MY3.

References

[1] G. H. Zeng and C. H. Keitel, "Arbitrated quantum-signature scheme," *Physical Review A*, vol. 65, no. 4, p. 042312, 2002.

[2] T. Hwang, S. K. Chong, Y. P. Luo, and T. X. Wei, "New arbitrated quantum signature of classical messages against collective amplitude damping noise," *Optics Communications*, vol. 284, no. 12, pp. 3144–3148, Jun. Jan. 2011.

[3] D. Gottesman and I. Chuang, "Quantum digital signatures," arXiv:quant-ph/0105032v2, 15 Nov. 2001.

[4] Y. G. Yang and Q. Y. Wen, "Arbitrated quantum signature of classical messages against collective amplitude damping noise," *Optics Communications*, vol. 283, no. 16, pp. 3198–3201, Aug. 2010.

[5] S. K. Chong, Y. P. Luo, and T. Hwang, "On "arbitrated quantum signature of classical messages against collective amplitude damping noise"," *Optics Communications*, vol. 284, no. 3, pp. 893–895, Feb. 2011.

[6] M. Curty and N. Lütkenhaus, "Comment on "arbitrated quantum-signature scheme"," *Physical Review A*, vol. 77, no. 4, p. 046301, 2008.

[7] G. H. Zeng, "Reply to "comment on 'arbitrated quantum-signature scheme"'," *Physical Review A*, vol. 78, no. 1, p. 016301, 2008.

[8] Q. Li, W. H. Chan, and D.-Y. Long, "Arbitrated quantum signature scheme using bell states," *Physical Review A*, vol. 79, no. 4, p. 054307, 2009.

[9] Y. G. Yang and Q. Y. Wen, "Erratum: Arbitrated quantum signature of classical messages against collective amplitude damping noise," *Optics Communications*, vol. 283, no. 19, p. 3830, Oct. 2010.

[10] J. Wang, Q. Zhang, L. M. Liang, and C. J. Tang, "Comment on: "arbitrated quantum signature scheme with message recovery"," *Physics Letters A*, vol. 347, pp. 262–263, 2005.

[11] H. Lee, C. Hong, H. Kim, J. Lim, and H. J. Yang, "Arbitrated quantum signature scheme with message recovery," *Physics Letters A*, vol. 321, pp. 295–300, 2004.

[12] J. Wang, Q. Zhang, and C. J. Tang, "Quantum signature scheme with single photons," *Optoelectronics Letters*, vol. 2, no. 2, pp. 209–212, May 2006.

[13] X. J. Wen and Y. Liu, "Authentic digital signature based on quantum correlation," arXiv:quant-ph/0509129v2, 11 Dec. 2006.

[14] X. J. Wen and Y. Liu, "Quantum message signature scheme without an arbitrator," in *The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007)*, Chengdu, China, 01-03 Nov. 2007, pp. 496–500.

[15] X. Zou and D. Qiu, "Security analysis and improvements of arbitrated quantum signature schemes," *Physical Review A*, vol. 82, no. 4, p. 042325, 2010.

[16] Q. Y. Cai, "Eavesdropping on the two-way quantum communication protocols with invisible photons," *Physics Letters A*, vol. 351, pp. 23–25, 2006.

[17] F. G. Deng, P. Zhou, X. H. Li, C. Y. Li, and H. Y. Zhou, "Robustness of two-way quantum communication protocols against Trojan horse attack," e-print quant-ph/0508168, 2005.

[18] P. O. Boykin and V. Roychowdhury, "Optimal encryption of quantum bits," *Physical Review A*, vol. 67, no. 4, p. 042317, 2003.

[19] M. Curty, D. J. Santos, and E. Perez, "Qubit authentication," *Physical Review A*, vol. 66, no. 2, p. 022301, 2002.

[20] H. Barnum, C. Crepeau, and D. Gottesman, "Authentication of quantum messages," in *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, Vancouver, BC, Canada, 16-19, Nov. 2002, p. 449.

[21] P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, "New high-intensity source of polarization-entangled photon pairs," *Physical Review Letter*, vol. 75, no. 24, pp. 4337–4341, Dec. 1995.

[22] H. Buhrman, R. Cleve, J. Watrous, and R. Wolf, "Quantum fingerprinting," *Physical Review Letter*, vol. 87, no. 16, p. 167902, Oct. 2001.